UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the matter of the search of
TARGET DEVICE 1, LOCATED IN THE EVIDENCE VAULT OF BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES - ST. LOUIS, FUTHER DESCRIBED IN ATTACHMENT A.

Case No. 4:24 MJ 7220 SPM

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, Duane Clauer, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 844(i) & 844(h)(1) 18 U.S.C. §§ 844(n) & 844(m) 18 U.S.C. §§ 844(h)	Use of fire to destroy any building affecting interstate commerce; Use of fire to commit a federal felony; Conspiracy to commit arson; Conspiracy to commit 18 U.S.C. §844(h)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

DUANE CLAUER Digitally signed by DUANE CLAUER Date: 2024.08.26 19:52:31 -05'00'

Applicant's signature

Special Agent/CFI Duane Clauer

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 08/28/2024

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: FINLEN

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF TARGET DEVICE 1, LOCATED IN THE EVIDENCE VAULT OF BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES - ST. LOUIS, FUTHER DESCRIBED IN ATTACHMENT A.	))))))	No. 4:24 MJ 7220 SPM FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Duane Clauer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – an electronic device – described in Attachment A, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. The affiant is a Special Agent/Certified Fire Investigator (SA/CFI) with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and has been employed by ATF since July of 2013. The affiant is currently assigned to ATF's Fairview Heights Field Office and his primary investigative focus is fire investigation. Prior to focusing on fire investigation, the affiant investigated violations of federal and state firearm and controlled substance laws, including violations under Title 18, United States Code, Sections 922 and 924, and Title 21, United States Code, Sections 841 et seq. From 2012-2013, affiant was employed as an agent with the Wisconsin Department of Justice, Division of Criminal Investigation. From 2008-2012, affiant was employed as a Wisconsin State Trooper, where he often seized controlled substances and firearms during highway patrol. The affiant has authored and executed both state and federal

search warrants in multiple judicial districts. The affiant has aided in the execution of search warrants of personal residences, vehicles, and commercial properties for evidence relevant to ongoing criminal investigations.

3. The affiant has attended the Federal Law Enforcement Training Center's Criminal Investigator Training Program and ATF's Special Agent Basic Training (SABT). Prior to employment with ATF, the affiant was a police officer in Wisconsin. The affiant has received advanced training in fire and explosion investigation at both the National Fire Academy and the National Center for Explosives Training and Research. The affiant has also received a Graduate Certificate in Forensic Arson and Explosion Investigation. Based upon the affiants training, experience, and consultation with other agents and law enforcement officers he knows that it is common for individuals involved in wire fraud and the destruction of property by fire to conceal their crimes/evidence in physical or digital form within financial documents, insurance documents, tax documents, and correspondence.

4. During the course of my law enforcement career, I have participated in numerous investigations involving fires, controlled substances, and firearms offenses. I have also conducted a variety of investigations of the trafficking and distribution of illegal narcotics. These investigations have led to the seizure of narcotics, weapons, and United States Currency. I am familiar with and have used various methods of investigations which include electronic surveillance, interviews of suspects and witnesses, search warrants, arrest warrants, and the handling of confidential informants.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. 844(i)- Use of fire to destroy any building affecting interstate commerce, 18 U.S.C. 844(h)(1)- Use of fire to commit a federal felony, 18 U.S.C. 844(n)- Conspiracy to commit arson, and 18 U.S.C. 844(m)- Conspiracy to commit 18 U.S.C. 844(h) have been committed by Jeffrey Cooksey or other persons known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

7. The information contained in this Affidavit is submitted for the sole purpose of demonstrating probable cause exists to search the following electronic devices (hereinafter collectively the "**subject electronic device**"), described below, and described and depicted in Attachment A:

a. **Device #1:** Silver cellular phone with AT&T emblem on it with a cracked screen and clear tape on one side of the phone which is listed as Exhibit 12 for ATF Case Number 24-18950.

8. Following their seizure, as described below, the **subject electronic device** was stored securely at the ATF St. Louis evidence vault, within St. Louis City, in the Eastern District of Missouri. Upon seizing **subject electronic device**, your Affiant observed the device to be in the off position. The **subject electronic device** has not been examined or altered in any way since the seizure.

9. The applied-for warrant would authorize the forensic examination of the **subject electronic device** for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth.

b. Subscriber Identity Module ("SIM") card: A SIM card is a smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing operation if removed. A SIM card is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital

data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This

removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

g. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication Devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

h. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

i. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control

a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

j. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

11. Based on my training, experience, and research, I know **subject electronic device** have the capabilities allowing it to serve as a **wireless telephone, digital camera, portable media player, GPS navigation Device, and PDAs**. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence which reveals or suggests who possessed or used the **subject electronic device**.

PROBABLE CAUSE

12. The following is only a partial summary of the information developed as a result of an investigation by your affiant, other ATF agents, and law enforcement officers in order to establish probable cause in support of this search warrant.

13. On July 15, 2024, ATF became involved in an investigation regarding several rental property fires in the Kennett, MO area in Dunklin County, MO. Several of the fires were found to be incendiary fires, and dealt with a group of landlords that knew each other and had the properties insured though the same insurance agent.

14. Your affiant became aware that a new ordinance passed in Kennett, MO that will go into effect on January 1, 2025 that will now require landlords to have their rental property

inspected and obtain an occupancy permit prior to renting. It was relayed to your affiant that many of the fires that have occurred were in properties that would likely not pass inspection and be costly to repair. It was also found that insurance claims were placed on these properties to collect insurance payouts following the fires.

15. Investigators discovered that Riley Cook DOB: 05/XX/82 who owns RCOOKPROPERTIES LLC has had at least eight (8) fires involving rental units and insurance claims since March 9, 2020. Many of those units were in poor condition and would have resulted in expensive repairs to pass the new inspections starting January 1, 2025.

16. Investigators discovered that Jeffrey Cooksey DOB: 05/XX/84 and Clayton Barnes DOB: 09/XX/71 did maintenance work for Riley Cook at his various properties.

17. Your affiant interviewed Clayton Barnes at the Ste Genevieve County Jail located at 5 Basler Dr, Ste Genevieve, MO on August 9, 2024. Barnes was read his statement of rights and waived his rights agreeing to talk to investigators.

18. Barnes worked for Cook from November 2023 until he was arrested on August 8, 2024, on a federal arrest warrant involving drug distribution. Barnes stated that Jeffrey Cooksey was also a maintenance man for Cook. Barnes stated that Cooksey has told him that he does "night work" for Cook, which Barnes took to mean setting fires based off the conversation they had. Barnes further stated that Cooksey stated he had some leverage against Cook for some "mysterious fires" and stated that Cook may have deleted his messages, but Cooksey kept them on his phone for leverage. Barnes stated when the conversation happened Cooksey held up his phone to show Barnes, although Barnes did not read the messages.

19. On August 9, 2024, your affiant interviewed Jeffrey Cooksey at the Dunklin County jail located at 1175 Floyd St, Kennett, MO 63857. Cooksey was read his statement of

rights and waived his rights agreeing to talk to investigators. Cooksey stated he worked for Riley Cook from September 2023 to around February of 2024. Cooksey stated he was living in one of Cook's rental properties during this timeframe at 2008 Blair Street, Kennett, MO. Cooksey stated that Cook would tell him to, "Put lipstick on a pig" when referring to repairs. Cooksey described many of the properties as being in poor condition with bugs and other issues with the houses.

20. Cooksey provided one of his cellular phone numbers as 573-551-1274 and provided Cook's number as 573-344-0492. Cooksey provided his most recent number as 573-344-6060, and stated his service is through AT&T. Cooksey stated the phone with the 6060 number was at his mom's house and he had his mom wipe the phone before giving it back to his girlfriend Crystal Reagan DOB: 06/XX/1986. Cooksey provided his moms address as 902 Court Street, Kennett, MO 63857.

21. Investigators asked Cooksey about doing "night work" for Cook. Cook responded that he would often go out at night for service calls for Cook when needed. Cooksey became very confrontational when asked about committing arsons for Cook. Cooksey denied setting any fires, and stated he had to use the restroom and wanted to end the interview with Investigators.

22. Investigators spoke to Cooksey's mother Rebecca Cooksey DOB: 7/XX/63 at 902 Court Street, Kennett, MO 63857. She confirmed that Crystal Reagan picked up the phone assigned call number 573-344-6060 from her. Rebecca Cooksey denied wiping the phone and stated she wouldn't know how to get in the phone to wipe it.

23. On August 14, 2024, your affiant interviewed Crystal Reagan at the Clay County Jail located at 268 South 2nd Street, Piggott, AR 72454. Reagan was read her statement of rights

and waived her rights agreeing to speak to investigators. Reagan stated she believed she started dating Jeffrey Cooksey around the April/May period of 2024.

24. Reagan stated when she started dating Cooksey that Cooksey was already terminated from his employment with Riley Cook. She stated that Cooksey allegedly used Cook's credit card to buy things that he wasn't supposed to buy. She stated that Cooksey was a maintenance man for Riley Cook. She provided Cooksey's most recent number as 573-344-6060 and her number as 573-344-0060. She stated she bought both phones when they started dating, and that's why she retrieved the phone with the 6060 number from Cooksey's mother. She stated when she received the phone it was already wiped by Cooksey's mother and the sim card was missing.

25. Reagan stated that Cooksey was extremely upset about getting fired from Riley Cook because he started fires for Cook. She stated that Cooksey's nickname is "Bubba". Reagan believed that Cooksey was responsible for several fires involving Cook's properties. She stated when she was arrested her mom Tammy Bridges went to her house at 2008 Blair Street to retrieve her property. She found out after the fact that her mom accidentally took one of Cooksey's phones which had a cracked screen. The phone was mixed in with Reagan's clothes. She described the phone as a silver back and having clear tape down one side of the phone. She stated that Cooksey used the phone to talk to other girls. She further provided the password to the phone as lili. She stated that was the initials of Cooksey's previous girlfriend Lindsey Ingram.

26. On August 14, 2024, your affiant went to 293 S. Main Street, Bragg City, MO to interview Tammy Bridges the mother of Crystal Reagan. Bridges stated she still had the phone that she retrieved from 2008 Blair Street in which she didn't know was Cooksey's phone. She

stated that she hasn't used the phone, and in fact the phone was turned off. Bridges signed a receipt of property and turned the phone over to your affiant.

27. On August 15, 2024, the cellular phone was entered into the ATF Saint Louis Group II Evidence vault as item 12 for ATF Case Number 24-18950.

What and Why Targets use Electronic Devices like the Subject Electronic Device

28. During your Affiant's career as a law enforcement officer, your Affiant has conducted numerous fire/drug/firearm investigations including those of drug trafficking organizations. Based on your Affiant's training and experience in such investigations, including electronic surveillance investigations, your Affiant and other members of the investigative team, know that individuals communicate with each other utilizing cellular telephones and other electronic devices to facilitate the overall scheme of their illicit endeavors. For instance, in order to be successful, drug traffickers must communicate via telephones or other electronic devices to orchestrate the importation of controlled substances; to manage and maintain contact with drug couriers; to maintain contact with lower-level distributors in their day-to-day operations; to maintain contact with safe house operators where narcotics are stored; and to coordinate the return movement of the drug derived profits back to the sources of supply.

29. Your Affiant knows from prior investigations and subsequent de-briefing of involved parties by investigative team members, that information obtained on cellular phones will often assist in identifying the user of that cellular device. In this instance, the phone was recovered from a residence of a family member who stated the phone belonged to Cooksey. Furthermore, a coworker believed that Cooksey had messages on his phone from Riley Cook about burning properties. Information on the phone could indicate others who may have known about the fires or the planning of setting the fires.

30. Your Affiant also knows in order to make it easier for individuals to communicate with one another, their phones and other devices often contain stored telephone numbers, programmed names, addresses, and encrypted codes and names. The phones often contain voicemails, text messages, photographs and emails relating to communications with co-conspirators, meeting locations as well as the telephone numbers of co-conspirators who have called or been called by the device.

31. Individuals engaged in the activities described in this affidavit use electronic devices and mobile phones for a variety of reasons including:

(a) accessing mapping and location services to assist in planning and facilitating their crimes, and to plan for their escape from crime scenes. Location data can indicate the user's patterns of behavior such as their physical location at the time the incidents occurred, and immediately prior to or after such incidents. It may also provide data related to the location of confederate's residences, safe houses or other places used to perpetrate the crimes.

(b) accessing contact lists of associates, confederates, and third parties;

(c) Targets take pictures and videos of themselves and associates, to memorialize their activities and fruits of their illicit activities such as contraband, firearms, and illegally obtained currency. They use the images or to brag to other confederates. These individuals frequently maintain these photographs on their electronic devices and, as described below, often post the images on social media.

(d) criminals use the devices for online social media platforms such as Facebook, Twitter, Snapchat, etc. They communicate with their associates and confederates over such

platforms. They post and display images and videos of contraband, fruits of their crimes, wealth, and otherwise memorialize criminal activities.

32. In summary, electronic devices such as the **subject electronic device** described herein and the services, they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society. Thus, there is reason to believe that Cooksey had, and used, the **subject electronic device** in conjunction with the events described herein. The **subject electronic device** themselves operate as instrumentalities of the crimes described herein.

What Can Be Recovered From the Electronic Devices

33. Based on training and experience, your Affiant knows that forensic examinations may be performed on electronic devices such as mobile phones tablets and, computers. Devices use internal fixed memory, SIM cards, or removable memory that stores the previously described information. It takes specialized training and experience along with software and hardware to perform forensic examinations and analysis of such devices and memory to retrieve this information. A forensic examiner may be able to recover evidence of the illegal activities described in this affidavit, including: user attribution, photographs, text messages, videos, phone and address books, call history, and geographical location data.

34. Further, electronic devices such as those identified in this affidavit can store information for long periods of time. These devices contain files or remnants of files that can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered

months or years later using forensic tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device.

35. Information that is electronically stored on the **subject electronic device** serves as direct evidence of the crimes described in this warrant. Forensic analysis may demonstrate how the **subject electronic device** were used, the purpose of their use, who used them, and when. There is probable cause to believe that such evidence will be on each of the respective **subject electronic device**. Data on the **subject electronic device** will likely also show who used or controlled the **subject electronic device**. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Lastly, data on the **subject electronic device** can show how the **subject electronic device** were used as an instrumentality of the crimes.

36. The **subject electronic device** have remained in the lawful possession of the ATF**,** since their seizure as described above. Therefore, while investigators might already have all necessary authority to examine **subject electronic device**, your Affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the **subject electronic device** will comply with the Fourth Amendment and other applicable laws.

37. In my training and experience, I know that **subject electronic device** have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **subject electronic device** first came into the possession of law enforcement.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

38. Based on knowledge, training, and experience, your Affaint knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed

via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

39. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **subject electronic device** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

40. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant applying for would permit the examination of the **subject electronic device** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

42. Your Affiant submits this affidavit supports probable cause for a search warrant authorizing the examination of the **subject electronic device** described in Attachment A to seek the items described in Attachment B.

43. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

44. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. Sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation

will be searched at this time. Based upon my training and experience, your Affiant has learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

I state under penalty of perjury the forgoing is true and correct.

Respectfully submitted,

DUANE CLAUER Digitally signed by DUANE CLAUER Date: 2024.08.26 19:53:01 -05'00'

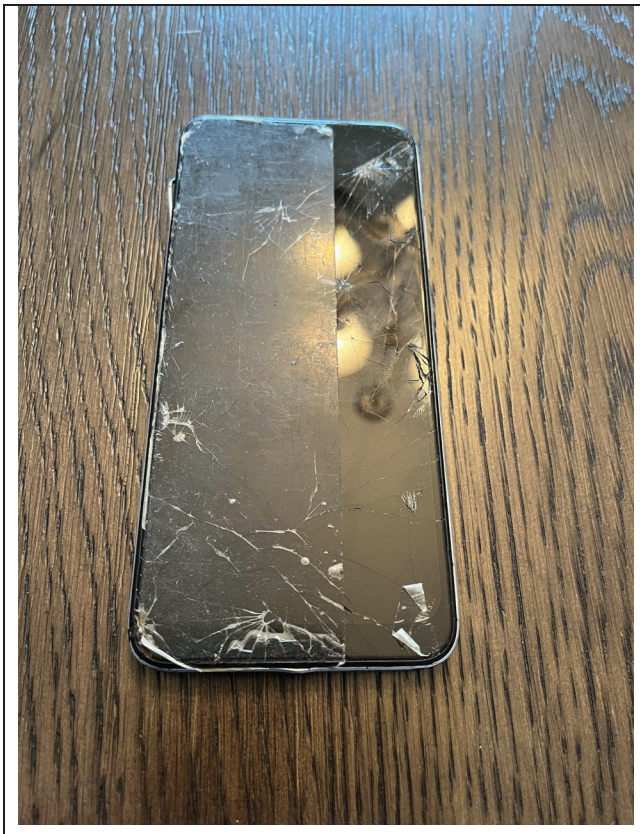
Duane Clauer
Special Agent/Certified Fire Investigator
Bureau of Alcohol, Tobacco, Firearms, and Explosives

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 28th day of August, 2024.

HONORABLE SHIRLEY P. MENSAH
UNITED STATES MAGISTRATE JUDGE
Eastern District of Missouri

ATTACHMENT A

A. Device #1: Silver cellular phone with AT&T emblem on it with a cracked screen and clear tape on one side of the phone which is listed as Exhibit 12 for ATF Case Number 24-18950

	
Front	Back

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. 844(i)- Use of fire to destroy any building affecting interstate commerce, 18 U.S.C. 844(h)(1)- Use of fire to commit and federal felony, 18 U.S.C. 844(n)- Conspiracy to commit arson, and 18 U.S.C. 844(m)- Conspiracy to commit 18 U.S.C. 844(h) and involve Jeffrey Cooksey and others known and unknown, including:

   a. Lists of co-conspirators identified on the phone.

   b. Any information including text messages, photos, videos, and internet searches regarding fires;

   c. Any information recording Cooksey's past travel and residence;

   d. All bank records, checks, credit card bills, account information, and other financial records that show a possible home residence to include purchases of items that can be used to commit arson.

   e. Any information related to fire or planning to commit a fire.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.